of specific disclosures of each reference. However, it is well settled that the proper inquiry for obviousness is what the reference as a whole teaches or suggests to those of ordinary skill in the art. It is impermissible to pick and choose among the features disclosed or taught by the prior art in determining obviousness.[1] Here, Campbell teaches a warning system for detection of network intrusion and misuse, while Hyman discloses a security system to control user's access and operations over data. That is, Campbell concerns only with a warning system, to alert the network administrators that an intrusion or misuse of the system may have occurred. Campbell system merely monitors network operations and reports on suspicious operations. It does not stop or prevent any of these operations, but is rather only an "alarm" system. Hayman, on the other hand, concerns with prevention of virus infestation, not network intrusion. To prevent the operation and spread of viruses, Hayman's system imposes restrictions on users' access to files and to various computer functions and data. Hayman teaches to assign different privileges to each user, depending on the user's job, and permitting the user to access only functions having compatible privilege level.

As can be readily ascertained from the above, none of the cited references or any combination thereof discloses or suggests the claimed invention. The claimed invention is a system that utilizes trust groups and object types for protection of computers, irrespective of users' privileges. Applicant respectfully submit that nothing in Campbell, Hayman, or any combination

[1] "It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position to the exclusion of other parts necessary to a full appreciation of what such reference fairly suggests to one skilled in the art." Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, 796 F.2d 443, 488, 230 U.S.P.Q. 416, 419 (Fed. Cir. 1986), citing In re Wesslau, 353 F.2d 238, 241, 147 U.S.P.Q. 391, 393 (CCPA 1965), cert. denied, 484 U.S. 823 (1987).

thereof even remotely suggests such a system. Nevertheless, Applicant provides herein a detailed response to the points made in the pending office action.

With respect to claims 1 and 13, it is alleged that Campbell discloses the limitation:

> "defining at least two trust groups, each of the defined trust groups
> being characterized by a trust group value"

Specifically, it is alleged that the gauges depicted in Figure 5a are the trust groups and the threshold of Figure 5a are the trust group values. It is respectfully submitted that even the broadest reading of the subject limitation cannot be made to cover such an interpretation. As clearly stated by Campbell in explaining Figure 5a, the gauges merely count the number of events of a particular type assigned to the particular gauge.[2] The gauges do not indicate a trust group and have no associated trust value. On the other hand, the thresholds are not trust group values, but rather indicate the level of activity of a user with respect to certain function of the computer. That is, Campbell's system uses a Boolean indicator, called criteria, to monitor user activity. A criteria is turned on (i.e., value = true) when an associated threshold has been passed.[3] Therefore, it can be understood that the gauges are not the claimed trust groups, the thresholds are not the claimed trust group values, and the gauges and threshold of Campbell do not disclose or suggest the trust groups that are characterized by trust group values.

[2] "Gauges are the mechanism used by the SI&W Engine 300 to measure key SI&W events ... Individual gauges may be either counters or statistical measures." Col. 16, Ln. 46-52.

[3] "Each criterion also has an associated threshold value that is used to trigger the criterion. For example, if the triggered criterion is linked to a counter gauge, it indicates that a certain type of activity occurred and that its occurrence exceeded an established level of concern as defined by its threshold value. If the threshold value was one, then a single occurrence will trigger the criterion. If the threshold value was five, then five occurrences within the specified interval of the gauge will trigger the criterion." Col. 18, ln. 52-61.

It is further alleged that the limitation

> "assigning objects and processes in the computer to one of said trust groups, irrespective of the rights of a user of said computer"

is disclosed by the assignment of events and gauges of Figure 5a. However, the audit events of Figure 5a are not objects and processes, but rather a record of a user activity.[4] Moreover, Campbell clearly teaches that the events and gauges are operated with respect to the user of the computer. See, e.g., Col. 5, ln. 63-65: "A gauge set is associated with every monitored user and machine in the monitored network environment."

Campbell's passage on column 13, lines 12-24 is cited as disclosing the limitation:

> "defining an action rule for each combination of process trust group value, object trust group value, and object type"

However, to begin with, as admitted in the pending Office Action, Campbell fails to disclose the limitations "defining at least two object types" and the limitation "assigning an object type to each of the objects." Since Campbell fails to disclose object types, clearly Campbell also fails to disclose action rules based in part on object type. Moreover, as shown above, Campbell also fails to disclose trust groups and trust group values. Therefore, Campbell fails to disclose the limitation of action rules based on the trust group and trust group value.

Finally, with respect to Campbell, it is alleged that it discloses the limitation:

[4] "User activity is a series of user actions within the monitored computer network environment, as represented by a stream of audit events". Col. 5, ln. 5-8.

> "upon an access request by a requesting process to a target object, performing the action indicated by the action rule applicable to the trust group value of the requesting process, the trust group value of the target object, and the object type"

This, of course, is not the case. Campbell is not concerned at all with access requests and does not disclose performance of any action in response to an access request.

It is further alleged that on column 2, lines 39-41, Hayman teaches "defining at least two object types and assigning an object type to each of the objects." Applicant respectfully submits that this is not so. In the cited passage, Hyman merely provides the definition of "objects." Applicant never intended to claim the invention of an object and the claim does not attempt to do so. What is claimed is the idea of defining different object types and assigning an object type to each object in the computer. There is nothing in Hyman that even remotely suggests this feature.

Therefore, as can be seen from the above, nothing in the cited references or any combination thereof provides the limitations of claims 1 and 13 and, accordingly, claims 1 and 13 and all claims dependent therefrom are allowable. That is, Applicant traverses the rejections of claim 2-6, 8-12, 14-16, 19, and 21, at least for their dependency on allowable claims 1 and 13.

Similarly, claim 23 and its dependent claims are allowed over the cited art and any combination thereof. While it is alleged Campbell modified by Hyman teaches the recited limitations of claim 23, this is clearly not the case. For example, it is alleged that in Figure 5b and column 13, lines 12-24, Campbell discloses "a list of rules, each rule defining an action based on an object type." However, this is not the case. Campbell explains its Figure 5b on column 20, lines 1-9, where Campbell explicitly states that the rules define logical relationship between the various criteria so as to determine the Boolean value of the respective indicators.

While it may be argued that the rules define actions (i.e., whether a Boolean value is TRUE or FALSE), the action does not depend on an object type. As Campbell discuss in his example, Indicator 1 is associated with a rule that it is turned on when either Criteria A or Criteria B is true. However, nothing in Campbell's disclosure teaches or even remotely suggests that this decision should depend on an object type.

It is also alleged that Campbell discloses "a list of trust groups, each trust group defining an object trust value and coupled to at least one of said rules. The support for this assertion is the same Figure and passages as were quoted for the similar limitation in claims 1 and 13. However, as explained in details above, Campbell does not disclose nor suggest these claim limitations. That is, as explained above, the gauges cannot be reasonably construed as trust groups and the thresholds cannot be reasonably construed as trust group values. Moreover, the Examiner failed to indicate how and where Campbell discloses the limitation "coupled to at least one of said rules."

It is further alleged that Campbell discloses "a plurality of objects, each of said objects having an object type and assigned to one of said trust groups." It is alleged that the events in Figure 5a of Campbell are the objects, and that they are assigned to gauges. As shown above with respect to claim 1 and 13, the events cannot be said to be the objects. Moreover, this limitation further requires that "each of said objects [have] an object type." The Examiner failed to show where in Campbell such a limitation is disclosed or suggested.

While it is alleged that Hayman teaches "a list of object types and assigning objects to an object type" this is clearly not the case. In the cited passage, on column 2, lines 39-41, Hayman merely defines the term "object." Hayman does not disclose object types, nor does he teach assigning objects to object types. Therefore, Hayman does not remedy the deficiencies of Campbell and no combination of the two references can be made to make the claimed invention obvious. Therefore, it is respectfully submitted that claim 23 and its dependent claims are all allowable. That is, Applicant traverses the rejections of claim 24 and 26, at least for their dependency on allowable claim 23.

While Applicant provided a detailed response traversing the rejections pending in the subject office action, Applicant notes that the rejections were made by selectively lifting various disclosures from the prior art and applying these disclosures devoid of any context to various claim limitations. That is, the Examiner has not considered the invention as a whole. The Examiner has primarily applied references which allegedly teach individual features of the present invention. It is well settled that a claim must be read as a whole, rather than element by element. See Ball Corporation v. US, 729 F.2d 1429, 221 U.S.P.Q. 289 (Fed. Cir. 1984). Moreover, as shown by Applicant, the cited references even fail to teach the individual features of the claims as alleged.

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

Joseph Bach
Registration No. 37,771

SUGHRUE MION, PLLC
Telephone: (650) 625-8100
Facsimile: (650) 625-8110

MOUNTAIN VIEW OFFICE
23493
CUSTOMER NUMBER

Date: March 7, 2006

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this RESPONSE UNDER 37 C.F.R. § 1.111 is being facsimile transmitted to the U.S. Patent and Trademark Office this 7th day of March, 2006.

Mariann Tam